AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of New York

UNITED STATES OF AMERICA)
v.)
PETER FARNUM,) Case No. 1:17-mj-334-DJS
)
)
)
)
)
Defendant.)

DISTRICT COURT
N.D. OF N.Y.
FILED
JUL 25 2017
LAWRENCE K. BAERMAN, CLERK
ALBANY

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. On or about the date(s) of October 2015 through April 2016 in the county of Saratoga in the Northern District of New York the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)(A)	Receipt of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

This criminal complaint is based on these facts:
See attached affidavit.

☒ Continued on the attached sheet.

Complainant's signature

Dave Fallon, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: July 25, 2017

Judge's signature

City and State: Albany, New York

Hon. Daniel J. Stewart, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, David C. Fallon, having been first duly sworn, do hereby depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since May 1991. I am assigned to the Albany Division, Albany, New York. My assignments include investigating violations of federal law—specifically, violent criminal offenses against children, including those involving the sexual exploitation of children. Prior to my employment as a Special Agent, I was an attorney licensed to practice law in the State of Rhode Island.

2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7)—that is, I am an officer of the United States who is empowered by law to conduct investigations of offenses enumerated in Title 18, United States Code, Section 2516(1). As an FBI Special Agent, I am authorized to seek and execute federal arrest and search warrants for Title 18 criminal offenses, including offenses related to the sexual exploitation of minors in violation of Title 18, United States Code, Section 2251(a).

3. I make this affidavit in support of an arrest warrant and criminal complaint charging PETER FARNUM, hereinafter "FARNUM," with knowingly receiving child pornography using a means and facility of interstate and foreign commerce, and in and affecting such commerce, in violation of Title 18 United States Code, Section 2252A(a)(2)(A); and knowingly possessing child pornography that has been transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, in violation of Title 18 United States Code, Section 2252A(a)(5)(B).

4. The statements contained in this affidavit are based upon my investigation,

information provided by other law enforcement officers and FBI personnel, and on my experience and training as a Special Agent of the FBI. As this affidavit is being submitted for the limited purpose of securing an arrest warrant and criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that FARNUM has violated Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B).

Details of the Investigation

5. On April 25, 2017, your affiant received information that FARNUM, a deputy sheriff with the Saratoga County Sheriff's Office ("SCSO"), may have received and/or possessed sexually explicit images of minors in or around 2016. Your affiant was further advised that evidence of the receipt and possession of said images may be found on a hard drive that, at the time your affiant was made aware of the matter, was in the possession of a private computer-forensic examiner located in Montana.

6. On April 26, 2017, your affiant spoke with D.E.,[1] the owner and operator of a computer-forensic business located in Hamilton, Montana. D.E. advised your affiant that on or about April 18, 2017, she entered a contract for computer-forensic services with C.S. of Ballston Lake, New York. Specifically, C.S. advised D.E. that she was concerned with FARNUM's use of a family computer to view and download pornography. Upon entering into the contract for computer forensic services, C.S. shipped—via Federal Express—two hard drives to D.E. One hard drive was the one removed from the family computer; the other was an external hard drive that C.S. had purchased for use in copying files from the hard drive.

7. As requested, D.E. performed a forensic examination of the hard drive removed

[1] The names of third parties have been abbreviated throughout this affidavit. In each case, the full name is known to your affiant.

from the family computer. While reviewing the results, D.E. found hundreds of images recovered from the hard drive's unallocated space.[2] Some of these images, according to D.E., depicted minor females, approximately 7 to 8 years old, posing in a sexually explicit manner. D.E. described several of the images that she observed as depicting 7- to 8-year-old females sitting nude with their legs spread apart and displaying their genitalia to the camera in a lewd and lascivious manner. According to D.E., a certified digital forensic examiner, the location of the images in the hard drive's unallocated space meant that they had been either downloaded or copied from another source, stored on the hard drive, and then deleted. D.E. advised your affiant that she observed in excess of 100 of these types of image files. After observing these images, D.E. contacted an FBI field office in Montana. As a result, Montana-based FBI Special Agent Devantier took possession of the hard drives and entered them as evidence into the files of the FBI.

8. On April 28, 2017, your affiant interviewed C.S. in person regarding her request that D.E. forensically examine the hard drives.

9. C.S. advised your affiant that she is currently married to FARNUM, but that they separated in October 2015 and have remained separated since. Despite the separation, FARNUM had unlimited access to the marital residence in Ballston Lake, New York, from October 2015 to April 2016 in order to care for the minor children he and C.S. shared when C.S. was at work. C.S. continued to live in the home fulltime during that period.[3] On April 13, 2016, C.S. accessed FARNUM's user account on the family computer because of her suspicion that

[2] Unallocated space is where a computer operating system stores data that has been deleted but not yet overwritten by new data.

[3] Except as noted below, *see* Paragraph 18, no one else besides FARNUM, C.S., and their three children lived at the house from October 2015 through April 2016. Moreover, the family employed no housekeeper, nanny, or similar domestic helper during that period who may have had access to the family computer by virtue of his or her employment.

FARNUM was using the computer to download and view pornography. The account was password protected, but C.S. was able to access the account by using a password that she was familiar with because FARNUM had used the same password in other contexts. At that time, the computer was kept in a home office at the house in Ballston Lake. While searching the contents of FARNUM's user account, C.S. found numerous folders that appeared to contain images of adult pornography. While viewing the contents of some of these folders, the image files began to disappear. Believing that a wiping program was purposefully and irretrievably deleting content, C.S. shut down the computer in order to preserve what she had discovered. C.S. confronted FARNUM about her findings the next day. FARNUM responded, "You shouldn't have done that," apparently referencing C.S.'s accessing of FARNUM's user account. After confronting FARNUM about the pornography, C.S. removed the computer from the house and brought it to her place of work. C.S. subsequently stored the computer in her workplace office. It remained there—untouched and powered down (i.e., turned off)—until April 2017, at which time C.S. decided to have the computer examined to ascertain the extent of FARNUM's online viewing of pornography. C.S. sought the examination as part of a divorce and custody proceeding and out of a general concern about FARNUM around the three minor children whom she and FARNUM share. (The children are currently 6 years old, 4 years old, and approximately 18 months old.)

10. First, C.S. brought the computer and an external hard drive that she had purchased for copying files from the family computer to a computer-repair business in Albany, New York. C.S. explained to an employee of the business what she was looking to have done. Specifically, she requested a review of the family computer to discover the extent to which FARNUM had used it to download and view pornography. The computer-repair business took possession of the computer and reviewed it as requested. An employee of the business subsequently advised C.S. that the hard drive contained thousands of images and videos depicting adult pornography. The

business copied these items to the external hard drive provided by C.S., and advised C.S. that it did not want to be involved in the matter any further. Because C.S. did not want to view the pornographic images and videos herself, she searched online for further professional assistance. While searching, she came across D.E.'s website advertising computer-repair and forensic services. C.S. contacted D.E. and discussed what she was looking for. Thereafter, C.S. entered into a contract with D.E. to examine and analyze the hard drives. (C.S. also contracted to have D.E. examine and analyze the external hard drive for evidence that it was connected, by the Albany computer-repair business, to the hard drive from the family computer in order to verify that the images located on the hard drive taken from the family computer were in fact copied to the external hard drive.) C.S. shipped the hard drives to D.E. via Federal Express. Subsequently, C.S. was alerted to D.E.'s discovery of child pornography in the hard drive's unallocated space. C.S. then contacted her attorney and informed him of D.E's findings. The attorney, in turn, contacted the United States Attorney's Office to report what C.S. had told him. The USAO then contacted the FBI by way of your affiant.

11. The FBI in Montana transferred possession of the hard drives to the FBI Albany Field Office in early May 2017. After receiving the hard drives, your affiant applied for and received a search warrant from this Court on May 5, 2017, to forensically examine the hard drive from the family computer. The warrant authorized investigators to search the hard drive for evidence of the receipt and possession of child pornography.

Results of Forensic Examination of the Hard Drive

12. The forensic examination of the hard drive was conducted by a computer scientist employed by FBI Albany. Briefly summarized, the findings of the forensic examination include the following:

a. 1,573 artifact files that contain hash values that match the hash values of identified/known child pornography ("CP") images.[4]

b. More than 5,000 other artifact files that appear to depict minors engaged in sexually explicit conduct or posed in a sexually suggestive manner. These image files were not part of any known CP databases used for comparison (see footnote 2 below for more information).

c. 7,856 files deleted from the system with names that indicate these files were child pornography.

13. The majority of the files that matched known CP images (Paragraph 12(a), *supra*) were application data remnants in the RealPlayer program. The RealPlayer program automatically creates thumbnail image files of image files displayed—or "played"—within the program. The majority of the original files for which the thumbnails had been created were

[4] "Hashing" is the process of running a file or group of files through an algorithm to produce a new value. The properties of that value may vary depending on the use case of the algorithm. Some of the most common algorithms serve to hide data such that the original input can only be derived when a specific value such as a password is known. This is seen in your everyday password protected file. Other algorithms are designed to show similarity between files, sometimes called "fuzzy hashing." This might be useful if someone had 300 picture files and wanted to know which ones contained the most amount of sky blue. Lastly, algorithms exist that attempt to show that files are either identical or different. This use case is often implemented online to show that a supplied password matches a stored password, as well as in digital forensics to show that a copy of a file or drive is identical to a control, such as a known file of interest or an original copy of evidence.

The MD5 algorithm is this last type. It has a 128-bit hash value, meaning that the probability that any two different random files have matching MD5 hash values (an event referred to as a collision) is 1 in 2^{128}, or very, very unlikely. The FBI and other law enforcement use MD5 to create hash values of files that are either known to be child pornography or are similar enough to child pornography that they are of investigative interest to an examiner. When conducting an examination, a common method for quickly locating and quantifying the presence of child pornography is to hash every file on a target drive, and compare those values to a databases of child pornography or media of investigative interest. If any values are found to match, those matches would be reviewed manually to confirm that they are indeed matches, and areas where matches are found would likely become focal points for a search for similar material that isn't already part of the database.

In this case, the Access Data FTK Imager version 3.1.3.2 was used to create a hash value for every file on the evidence item. Those hash values were compared to databases containing hash values of known child pornography or media of investigative interest using Griffeye Analyze. Griffeye determined that there were 1,573 hash values that matched hash values in databases of known child pornography images, and 5,714 hash values that matched databases of files of investigative interest.

found to have been deleted. The thumbnails, however, constitute digital copies of the original images that are only different from the original in that they are lower resolution than the original.

14. The Windows account associated with the vast majority of the CP material was labeled "Pete." Of the 1,573 files that matched known CP hash values, 1,444 were found in file paths associated with this user account. (One file was found in the "C[.]" account; specifically, it was found in a deleted web-browsing artifact).[5] The remaining files were carved from backup or unallocated space.

15. Additionally, the forensic examination revealed several artifacts that appear to attribute the activities involving the possession and receipt of sexually explicit images of children to FARNUM. These artifacts, as more specifically detailed below, include the use of an email account associated with FARNUM, game saves for a computer game titled "Civilization IV: Beyond the Sword," and internet searches indicating an interest in Homeland Security post-graduate studies and combat tactical systems.

Timeline Analyses Indicating That FARNUM Used the Computer to Receive and Possess Child Pornography

16. The following table details a timeline analysis for events that occurred on the family computer (i.e., hard drive) on Monday, October 12, 2015, between 11:54 a.m. and 12:27 p.m. According to records obtained from the SCSO, FARNUM worked the midnight to 8 a.m. shift on October 12, 2015, and was not on duty from 11:54 a.m. to 12:27 p.m. Moreover, according to C.S.'s typical work schedule, she was at work at the time.

Time	Event	Source
15:54 UTC	Web visit to url: URL: https://webmail.saratogacountyny.gov/versions/webmail/11.6.1-	Database entry time,

[5] This second account shared the first name of C.S., whose full name is abbreviated throughout this affidavit.

	RC/sounds/notifier_05.mp3, Content Size (Bytes): 0, Record No: 10478	Item 1
16:20 UTC	Google search for "combined tactical systems fet"	Database entry time, Item 2
16:27 UTC	1 file of what appears to be a minor masturbating is imported by RealPlayer. This file is visually the same as the one imported on 1/7/2015.	File creation date, Item 3

Item	Path
1	[ROOT]\Users\Pete\AppData\Local\Google\Chrome\User Data\Default\Cache\index; File Offset 304. [ROOT]\Users\Pete\AppData\Local\Google\Chrome\User Data\Default\Cache\data_1; File offset 624128
2	[root]/System Volume Information/{aafd4727-00fe-11e6-89ae-d4856498a30e}{3808876b-c176-4e48-b7ae-04046e6cc752}. OS (Volume Shadow Copies) - Shadow Copy Creation Time: 2016-04-13 07:03:16 UTC (yyyy-mm-dd), Machine: Animal7, ID: {08e2216f-4ef2-4f7a-9f95- 1fe9e3698509}; File Offset 3434566749
3	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/494D7774940948E8_1444667271.JPG

This event depicts the user of the family computer accessing a webmail account hosted by "saratogacountyny.gov" at 11:54 a.m. (UTC - 4). Significantly, FARNUM's employment email address is "[xxxxxx]*@saratogacountyny.gov*" (emphasis added). At 12:20 p.m. (UTC - 4), the user accessed the search engine "Google" to search the term "combined tactical systems." Significantly, FARNUM is a member of the SCSO's Special Weapons and Tactics ("SWAT") Team. At 12:27 p.m. (UTC - 4), the user imported a file ("494D7774940948E8_ 1444667271.JPG") into the RealPlayer program. This file was reviewed by your affiant and found to contain a screen capture from the Internet-based website "omegle.com." The image depicts an approximately 10- to 13-year-old female lying on her back with her legs spread apart. She is using her hands to touch her vaginal area and appears to be masturbating.

17. The following table details a timeline analysis for events that occurred on the family computer on October 19, 2015, between 9:46 a.m. and 12:27 p.m. According to records obtained from the SCSO, FARNUM worked the midnight to 8 a.m. shift on October 19, 2015, and was not

on duty from 9:46 a.m. to 12:27 p.m. Moreover, according to C.S.'s typical work schedule, she was at work at the time.

Time	Event	Source
13:46 UTC	9 files flagged by Griffeye as being of investigative interest are imported into RealPlayer. These files appear to depict a minor; some depict the minor's exposed genitals.	File creation time, Items 1-9
14:08 UTC	Google search for "masters homeland security"	Database entry time, Item 10
16:27 UTC	Visited St. Josephs university's website page for their degree in homeland security.	Database entry time, Item 11

Item	Path
1	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/ 56EE963F5D976600_1445262420.JPG
2	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/ BF36DDAA8225E139_1445262413.JPG
3	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/ BF36DDAA8225E139_1445262412.JPG
4	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/ A39309273790E3EE_1445262407.JPG
5	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/ 59918859C366E0CE_1445262397.JPG
6	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/ 0E2CF3E0F9EA2664_1445262390.JPG
7	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/ 82A5C042E38009CB_1445262382.JPG
8	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/ 6341480659CF6A45_1445262375.JPG
9	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/ 65AC96E85F794D03_1445262365.JPG
10	[ROOT]\Users\Pete\AppData\Local\Google\Chrome\User Data\Default\Cache\index; File Offset 288 [ROOT]\Users\Pete\AppData\Local\Google\Chrome\User Data\Default\Cache\data_2; File Offset 11276288 URL: https://www.google.com/gen_204?atyp=i&ct=1&cad= 1&sqi=3&q=masters%20homeland%20security&oq= masters%20homeland%20securiloty&gs_l=hp.10..0l2j0i22i30l2. 74918.94445.0.94673.50.27.12.11.11.0.636.10387.0j12j5-15.27.0....0...1c.1.64.psy-ab..2.48.9130.viwBUy84f2s&ei=WfkkVuvrK4Ok jwPUrafQBg&zx=1445263741434
11	[ROOT]\Users\Pete\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3; File Offset 52240384

URL: http://www.sju.edu/int/academics/cas/grad/homelandsec/, Content Size (Bytes): 16356,

This event log shows that the user of the family computer imported images into the RealPlayer at 9:46 a.m. A review of these images found that they appear to depict an approximately 10- to 12-year-old female posed in various ways. With the exception of image 65AC96E85F794D03 _1445262365.JPG, each of the images depict this minor female displaying her naked vaginal area in a lewd in lascivious manner. At 10:48 a.m., the user conducts a "Google" search using the term "masters homeland security." According to C.S., whom I have interviewed about this timeline analysis, she never utilized the computer to search the internet for Master's programs in Homeland Security. C.S. supposed that FARNUM might have had an interest in such a program because it relates to his career in law enforcement.

18. The following table details a timeline analysis for events that occurred on the family computer on December 29, 2015, between 8:08 p.m. and 9:25 p.m. At the time these events occurred, C.S. was not home for a period of approximately three days and two nights. At that time, FARNUM had access to the home and was at the home to visit and care for two of his and C.S.'s children. (Your affiant is informed that C.S.'s parents also had access to the house for the brief period during which C.S. was not home.) According to SCSO records, FARNUM did not work on December 29, 2015.

Time	Event	Source
20:08 – 20:27 UTC	66 files flagged by Griffeye as matching known hash values for CP are imported into RealPlayer application data	File creation time, Items 1
20:30 – 21:25 UTC	12 files containing names that suggest they are CP are deleted from the RealPlayer table, with origin file metadata indicating they had originally come from the "\Users\Pete\Downloads\off\" directory.	Database entry time, Item 2

Item	Path
1	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/E636F7707D56B3BE_1451419737.JPG
2	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/library.db; "deleted_assets" table, id "18105", path "C:\Users\Pete\Downloads\off\lolitacastle_59_001_1.jpg"

This event log shows that the user of the family computer imported images into the RealPlayer starting at 8:08 p.m. on December 29, 2015. Your affiant has viewed a number of these images. The images depict minor females, all approximately 8 to 11 years old, posing naked with their legs spread and displaying their naked genitalia to the camera.

19. The following table details a timeline analysis for events that occurred on the family computer on December 31, 2015 between 11:04 p.m. and January 1, 2016 at 2:45 p.m.:

Time	Event	Source
4:04 – 4:56 UTC	1,758 files flagged by Griffeye as matching known hash values for CP are imported into RealPlayer application data	File creation time, Item 1
4:35 – 4:48 UTC	2,645 files containing names that suggest they are CP are deleted from the RealPlayer table, with origin file metadata indicating they had originally come from the "\Users\Pete\Downloads\SMLL54MS\SMLL54MS\SMLL54MS\Siterip My Little lolita 54 Models Sets" directory.	Database entry time, Item 2
13:01 - 17:14 UTC	7 videogame save files for the game "Civilization [IV]: Beyond the Sword" are created	File creation time, Item 3
19:15 – 19:18 UTC	462 files flagged by Griffeye as matching known hash values for CP are imported into RealPlayer application data	File creation time, Items 4
19:15 UTC	2,020 files containing names that suggest they are CP are deleted from the RealPlayer table, with origin file metadata indicating they had originally come from the "\Users\Pete\Downloads\SMLL54MS\SMLL54MS\SMLL54MS\Siterip My Little lolita 54 Models Sets" directory.	Database entry time, Item 5

Item	Path
1	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/ 63442E72B00C3925_1451621061.JPG
2	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/library.db; "deleted_assets" table, id "18835", path "C:\Users\Pete\Downloads\SMLL54MS\SMLL54MS\SMLL54MS\Siterip My Little Lolita 54 Models Sets\CrisNAda-100\crisnada001.jpg"
3	[NTFS]/[root]/Users/Pete/Documents/My Games/beyond the sword/Saves/single/Darkhorse V AD-1983.CivBeyondSwordSave
4	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/ 49DB0E32A5601380_1451675881.JPG
5	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/library.db; "deleted_assets" table, id "22870", path "C:\Users\Pete\Downloads\SMLL54MS\SMLL54MS\SMLL54MS\Siterip My Little Lolita 54 Models Sets\Viola_61\viola061.jpg"

The above timeline indicates that the user of the "Pete" account imported known child sexual exploitation images into the RealPlayer beginning at 11:04 p.m. on December 29, 2015 (UTC -5). The user subsequently deleted child pornography from the RealPlayer program. Further, several hours later, the timeline indicates that the user of the "Pete" account saved gaming activity ("Civilization IV: Beyond the Sword") seven times over the course of four hours. Two hours later, the user imported more known child sexual exploitation images into the RealPlayer program. Afterward, the user again deleted child pornography from the RealPlayer program. According to SCSO records, FARNUM was not on duty at the time of these activities. Moreover, according to C.S., FARNUM was then living at the Ballston Lake marital house helping with their three children.

20. According to C.S., she does not play "Civilization IV: Beyond the Sword" and, in fact, no one at the house used the computer to play any computer games besides FARNUM. Moreover, your affiant has determined that "Civilization IV: Beyond the Sword" is a turn-based strategy game that allows players to build civilizations following the invention of gunpowder. As described in Paragraph 10, *supra*, C.S. and FARNUM share children who, in and around

December 2015, were approximately 4 years old, 18 months old, and just born—all too young to have signed on and played the game themselves. *See, generally, Civilization IV: Beyond the Sword*, WIKIPEDIA.ORG, https://en.wikipedia.org/wiki/Civilization_IV:_Beyond_the_Sword (last visited July 24, 2017). Additional activity on the computer linking the "player" of "Civilization IV" to the importation of sexually explicit images of minors is present in the January 8, 2016 activity log below:

Time	Event	Source
18:43 – 18:45 UTC	669 files flagged by Griffeye as matching known hash values for CP are imported into RealPlayer application data	File creation time, Item 1
19:27 UTC	1 videogame save file for the game "Civilization [IV]: Beyond the Sword" is created	File creation time, Item 2
21:58 UTC	433 files containing names that suggest they are CP are deleted from the RealPlayer table, with origin file metadata indicating they had originally come from the "\Users\Pete\Downloads\LSM08_-_pic_sets\LSM08 - pic sets" directory.	Database entry time, Item 3

Item	Path
1	[NTFS]/[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content/images/00829E5244271E8A_1452278623.JPG
2	[NTFS]/[root]/Users/Pete/Documents/My Games/beyond the sword/Saves/single/Darkhorse V AD-2029-January.CivBeyondSwordSave
3	? real player asset database .... Number 26359 C:\Users\Pete\Downloads\LSM08_-_pic_sets\LSM08 - pic sets\01\LSM-001_001.jpg

Use of RealPlayer to View Child Pornography on the Computer

21. RealPlayer is a cross-platform media management program that allows users to consolidate their media library through one program. It also provides capabilities to download videos found via web browsing, play music or movies, share media with peers, cast media to supported devices, and sync media between a user's devices via cloud service. By default, RealPlayer will import media from a user's "Downloads," "Music," "Pictures," and "Videos"

folders. The computer scientist who performed the forensic analysis on the computer found the following information concerning the use of the RealPlayer program:

22. Windows Prefetch logs recorded the following statistics for RealPlayer:

Prefetchfilename_realplayerX			
Program	First Run	Last Run	Times Ran
RealPlayer	12/15/11 4:40PM	4/14/16 6:37PM	6840

According to the results of the forensic examination, RealPlayer stores thumbnails for content imported into the RealPlayer library on the computer at "[root]/Users/Pete/AppData/Local/Real/RealPlayer/Content." Microsoft Windows hides the AppData folder and its subfolders from users by default using a feature called "hidden files and folders" that is designed to protect users from meddling with elements that applications may rely on to operate, so an average Windows user may not have any idea that such a folder exists or what content is stored in it. Note that 1,388 of the 1,573 files whose hash values matched known CP were found in this location.

23. RealPlayer stores information about the media it finds in a database called "Library.db" located at "[root]/Users/%username%/AppData/Local/Real/RealPlayer/Library.db." One of the tables in this database, "deleted_assets," contains information about files that were deleted. This table was searched for certain filename strings that indicate a file may have been child pornographic material or of investigative interest. The search terms included the following:

- "Lolita" – Lolita complex refers to sexual attraction to younger girls
- "pthc" / "pt" / "ptc" - Pre-Teen Hard Core / pre-teen
- "LSM" – Little sex machine
- # "yo" – Years old, where "#" is any integer value lower than 18.
- "kidz" – Referring to kids.

In total, forensic analysis uncovered 7,856 filenames on the computer that matched the above

filters, suggesting that a large amount of child pornographic material had been viewed in RealPlayer and subsequently deleted.

Use of Cleaning and Recovery Programs on the Computer

24. In addition to the foregoing, two forensic programs of interest were found on the family computer during the forensic examination thereof by the FBI's computer scientist. One such program was CCleaner, a popular tool for cleaning up computers. (From the publisher's website: "CCleaner is the number-one tool for cleaning your PC. It protects your privacy and makes your computer faster and more secure!") This includes securely erasing files, browser history, and registry entries. While the software is not itself malicious, it could be used to destroy evidence of malicious activity. Prefetch logs indicated the following usage statistics for Ccleaner:

Prefetchfilename_ccleanerX			
Program	First Run	Last Run	Times Ran
CCleaner (file erasing)	4/14/16 1:59PM	4/14/16 2:16PM	6

25. The second forensic program found during the examination was Recuva, a popular tool for recovering deleted files. (From the publisher's website: "Recuva can recover pictures, music, documents, videos, emails or any other file type you've lost. And it can recover from any rewriteable media you have: memory cards, external hard drives, USB sticks and more!") Prefetch logs indicate the following usage of the program:

Prefetchfilename_recuvaX			
Program	First Run	Last Run	Times Ran
Recuva (file recovery)	4/14/16 1:59PM	4/14/16 2:05PM	3

26. The below table shows the metadata for a folder labeled "Rec," located at "/Users/Pete/Downloads/Desktop/Rec."

"Rec" directory metadata	
Location	"[root]/Users/Pete/Downloads/Desktop/Rec"
Created	4/14/2016 2:05:59 PM
Accessed	4/14/2016 2:22:47 PM
Modified	4/14/2016 2:22:47 PM

Note the following: The "Rec" folder was created at the same time as the last known runtime for Recuva, and contained 37 files that had hash values matching known child pornography image files. Thirty of these files were previously deleted from the "Rec" folder.

27. Based on the foregoing, your affiant believes that on April 14, 2016, in response to a discussion FARNUM had with C.S. about her discovery of pornography on the family computer on April 13, 2016 (*see* Paragraph 10, *supra*), FARNUM downloaded the Recuva and Ccleaner software (which may in fact have installed together as they are from the same publisher). CCleaner was first run on the computer on April 14, 2016; Recuva was run three times between 1:59 p.m. and 2:05 p.m. on that same day. When it was run, Recuva recovered a large amount of files that were placed into the "Rec" folder. As described above, 37 of those files had hash values matching known child-pornography image files. According to SCSO records, FARNUM did not work on April 14, 2016.

28. Your affiant reviewed the 37 files that were found inside the "Rec" file. Your affiant observed the following: These images depict minor females, approximately 9 to 13 years old, posing in a sexually explicit manner and engaged in sexual activity. For example, one image observed by your affiant depicts a minor female, approximately 9 to 10 years old, sitting in a chair, completely nude. Her legs are spread apart and drawn up toward her chest, thereby exposing her naked vaginal area in a lewd and lascivious manner. A second image depicts a minor female, approximately 8 to 10 years old, completely nude, straddling a nude adult male. The male's penis is inserted into the child's vagina.

Conclusion

29. Based upon the above information, there is probable cause to believe that FARNUM received and possessed child pornography between about October 2015 and April 2016 in the Northern District of New York.

WHEREFORE, I respectfully request that the Court issue a warrant for FARNUM's arrest and a complaint charging FARNUM with violation of Title 18, United States Code, Section 2252A(a)(2)(A), and violation of Title 18, United States Code, Section 2252A(a)(5)(B).

David Fallon, Special Agent
Federal Bureau of Investigations

Sworn to me this 25th day of July, 2017.

Hon. Daniel J. Stewart
United States Magistrate Judge